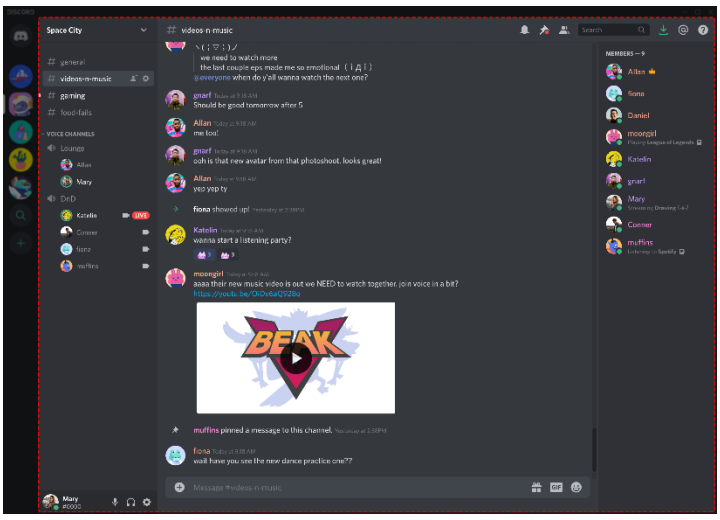
The Real(ly insecure) World

Uppgift för 220s CTF

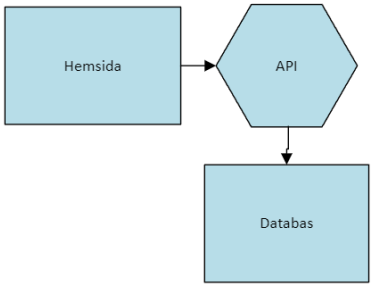
Simon Meier

Min CTF uppgift är inspirerad av hackningen av Andrew Tate’ s discord klon ”the real world.” Här är en rolig video om händelsen: [The Andrew Tate Hack is Worse than you Think... - YouTube]

Beskrivning av uppgiften



Jag kommer bygga en hemsida som ska ha samma utseende som discord. Du kommer vara inloggad som en användare som redan har varit aktiv och du har några vänner. Målet med uppgiften är att läsa privata chattar mellan dina vänner, där flaggan kommer att finnas.



Hemsidan kommer fungera rätt så simpelt. All data hämtas med en API från en databas på samma server där api’n körs. Svagheten kommer att finnas vid API’n.

API’n kommer använda sig av python biblioteket fastAPI som har Cross-Origin Resource Sharing (CORS) policies. Med hjälp av det kommer jag gör att bara min hemsida kan få tillgång till API’n. Den planerade svagheten ligger istället i att man kan modifiera API anropet från hemsidan genom en ”man in the middle” attack och på så sätt få API’n att ge tillbaka fel information (informationen med flaggan)

Tekniskt planerar jag att när hemsidan laddar in kommer den att hämta alla personens kompisar med hjälp av ditt id, (kommer vara hårdkodat). När alla kompisar har hittats kommer ett till API anrop göras där alla chattar med dina kompisar laddas in. Dessa kommer använda sig av en sårbar struktur, något liknande: ”api /chattar/user-id1:user-id2” där user-id1 är ditt och user-id2 är din kompis. Genom att då bytta ut ditt user-id med en annan kompis user-id för du tillgång till deras chattar och därför flaggan!

Målet är att använda nuxt och tailwind för att bygga hemsidan vilket är det jag är van vid och kommer därför kunna programmera snabbare.

Svårighetsgrad

Jag tror att svårighetsgraden ligger runt 0,8. Anledningen är för att det inte är så mycket man måste gör utan man ska bara ändra ett user-id för att ta sig till flaggan. Jag har det dock inte på 1 eftersom visa elever kanske inte har jobbat med API på länge (hösten i tvåan) och därför inte ser kopplingen.

Utvecklingspotential

Beroende på hur fort det går att programmera det jag planerat kan jag lägga till extra steg i uppgiften för att göra den svårare.